TENNESSEE DEPARTMENT OF FINANCE AND ADMINISTRATION
STS Director 2 - Deputy Chief Information Security Officer

Job Summary: Reports to the Chief Information Security Officer (CISO) within Strategic Technology Solutions, the Deputy Chief Information Security Officer (Deputy CISO) is responsible for assisting the CISO to establish and implement the information security governance structure and strategies, priorities, and directives consistent with the vision of the state. This position will function as a liaison between STS and state agencies to assist in the implementation of the state's security policies, processes, technologies, and practices and will act on behalf of the CISO in his or her absence.

Responsibilities:

- Provide recommendations to the CISO on information security standards and best practices for IT projects.
- Assist the CISO to oversee and manage the effectiveness of the state's security program.
- Coordinate with business partners to resolve complex or highly sensitive IT issues.
- Provide advice to operating units at all levels on information security issues, recommended practices, and vulnerabilities.
- Develop and deploy the security program for assigned areas to ensure policies, procedures, and objectives are closely aligned with those of the state.
- Assist in the development of metrics to measure the efficiency and effectiveness of the security program.
- Assist the CISO in strategy development and managing the information security program, focusing on security risk assessments; risk management (including risk prioritization and mitigation); education and awareness.
- Work with the CISO to ensure there is appropriate allocation of budgeted funds within assigned units so that the highest priority projects have sufficient monetary resources to be completed in a timely and efficient manner.
- Ensure policy and risk controls are in place, updated when necessary, and risks are communicated to the appropriate business owners.
- Direct the incident response planning and management of security incidents and events to protect State IT assets (e.g. information, critical infrastructure, intellectual property, and reputation) in addition to investigations of security breaches, and assist with disciplinary and legal matters associated with such breaches, as necessary.
- Provide oversight on vulnerability management, including, but not limited to maintaining a centralized scanning environment, identifying scan targets (hardware and web applications), listing and scheduling scans, and work with target owners to remediate identified vulnerabilities.
- Lead the disaster recovery program, including, but not limited to auditing and testing recovery plans, promoting the importance of disaster recovery and continuity planning to agencies, and the performance of business impact analyses.
- Interface with law enforcement agencies and other government agencies to address security lapses and responds to information security issues.
- Respond appropriately with resources and information to requests submitted by internal and external auditing functions.
- Collaborate with IT Management, Legal, Internal Audit and Human Resources in the development and implementation of policies, standards, procedures and awareness.
- Maintain relationships with local, state and federal law enforcement and other related government agencies.
- Maintain relationships with agencies and boards to establish and facilitate security and risk management processes, including the reporting and oversight of remediation efforts to address negative findings; identify acceptable levels of risk; and establish roles and responsibilities with regard to information classification and protection.
- Communicate with executive leadership to ensure appropriate technologies are in place to safeguard the state's infrastructure and data assets.
- Assign responsibilities to staff and empower employees to execute the security program.
- Develop job performance plans for assigned subordinates to communicate responsibilities and expected outcomes of performance in their role.
- Review and approve future staffing and skill requirements needed for succession planning and talent management purposes.

Minimum Qualifications: Bachelor's degree in an IT or Business related field. Relevant professional information technology experience may be substituted for the required degree.

- Eight years of experience in information technology, information security or risk management.

- Knowledge of information security standards and best practices.
- Knowledge of federal, state, and local laws, rules, regulations, policies and procedures, and best practices as they relate to information systems governance.
- Knowledge of regulatory guidance in security and risk management.
- Knowledge of Risk/Audit/Compliance competencies especially as it relates to security and risk management.
- Knowledge of technological trends and developments in the area of information security, governance, risk and compliance management, and data loss prevention.
- Knowledge of management of an effective security and compliance program, including training, monitoring, conducting and documenting investigations, addressing violations, and monitoring corrective actions.
- Knowledge of Security Incident Responses, Security Vulnerability Assessments, Penetration Testing, Auditing, and Security Awareness Training.
- Knowledge of infrastructure components, including infrastructure security components (e.g. network security, firewalls, IDS, IPS etc.).
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and non-technical audiences.
- Expert knowledge of strategic decision methodologies.
- Expert knowledge of management best practices.

Preferred Qualifications:

- Prior state government experience is a plus.

Knowledge, Skills, Abilities, Competencies:

- Decision Quality
- Business Acumen
- Problem Solving
- Customer Focus
- Innovation Management
- Priority Setting
- Drive for Results
- Building Effective Teams
- Conflict Management
- Delegation

The State of TN is an Equal Opportunity Employer.

Resumes should be submitted via email to EIT.Resumes@tn.gov

Pursuant to the State of Tennessee's Workplace Discrimination and Harassment policy, the State is firmly committed to the principle of fair and equal employment opportunities for its citizens and strives to protect the rights and opportunities of all people to seek, obtain, and hold employment without being subjected to illegal discrimination and harassment in the workplace. It is the State's policy to provide an environment free of discrimination and harassment of an individual because of that person's race, color, national origin, age (40 and over), sex, pregnancy, religion, creed, disability, veteran's status or any other category protected by state and/or federal civil rights laws.